DETAILED ACTION

Status of Claims

1. This Office Action is responsive to the amendment filed December 03, 2007.

2. Claims 1-17 are currently pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cook et al. (US Patent No. 6,675,153 B1) in view of Yacobi et al. (US Patent No. 7,020,638 B1).

Referring to claim 1, Cook et al. disclose a digest by performing a hash on the electronic fund transfer disbursement file (see at least abstract & col. 1, lines 24-41);

- receiving an authorization response from the remote system (see at least abstract & col. 2, lines 39-55);
- a web server system for transferring authorization control code to the remote system, the authorization control code driving the remote system to perform the following steps (see at least Fig. 4). In the fig. 4 shows the web server, which is well known to do this kind of operations.
- obtaining the digital signature of authenticated attributes, the authenticated attributes including the digest (see at least col. 2, lines 38-52); and

- generating the authorization response, the authorization response including the digital signature (see at least abstract & col. 2, lines 38-52).

Cook et al. does not expressly disclose a payment management system for obtaining approval of an electronic fund transfer disbursement file from a user of a remote system and transferring the electronic fund transfer disbursement file to a payments processor, the payment management system comprising: an electronic transfer submission module for; transferring an electronic funds submission to the payments processor, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising a digital signature;

Yacobi et al. discloses a payment management system for obtaining approval of an electronic fund transfer disbursement file from a user of a remote system and transferring the electronic fund transfer disbursement file to a payments processor, the payment management system comprising (col. 1, 5, lines 24-44, 50-57):

- an electronic transfer submission module for (see at least abstract & col. 5, line 50-57);
- transferring an electronic funds submission to the payments processor, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising a digital signature (see at least abstract col. 16, 18, lines 8-14, 54-67);

Therefore, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have modified of Cook et al. to include the step(s) taught by Yacobi et al. as discussed above in order to provide a real-time software application is provided that allows consumers to authorize transaction in a secure, private, and convenient manner for the purchase of goods and services over the internet (see at least col. 1, lines 52-56).

Referring to claim 2, Cook et al. discloses the digital signature comprises a digital signature of a hash of the authenticated attributes (see at least abstract & col. 1, lines 24-41);

- the authorization control code further provides for the remote system to, generate additional message attributes (see at least abst. & col. 1, lines 24-41);
- combine the additional message attributes with the digest to generate the authenticated attributes (see at least abst. & col. 1, lines 24-41);

Referring to claim 3, Cook et al. discloses generate and pass a dummy data string to a signing component to obtain a dummy authentication data structure, the dummy authentication data structure comprising a dummy digital signature (see at least abst. & col. 1, lines 14-49);

- pass the authenticated attributes to the signing component to obtain the digital signature (see at least abst. & col. 1, lines 14-49);
- combine the digital signature with at least a portion of the dummy authentication data structure by replacing the dummy digital signature with the digital signature to generate an authentication data structure (see at abst. & col. 1, lines 14-49);
- and include the authentication data structure in the authorization response (see at least abst. & col. 1, lines 14-49).

Referring to claim 4, Cook et al. discloses the dummy data structure further comprises a dummy digest (see at least abst. & col. 1, lines 14-49);

- the authorization control code further drives the remote system to combine the digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest (see at least abst. & col. 1, lines 14-49).

Referring to claim 5, Cook et al. discloses obtaining log on credentials identifying the user of the remote system; determining whether the log on credentials match those of an authorized user (see at least abst. & col. 1, lines 14-49);

- the electronic fund transfer submission module transfers the authorization request to the remote system only if the log on credentials match those of an authorized user (see at least abst. & col. 1, lines 14-49).

Referring to claim 6, Cook et al. discloses receiving an authentication challenge from the payments processor (see at least abst. & col. 1, lines 14-49);

- transferring the authentication challenge to the remote system (see at least abst & col. 1, lines 14-49);
- receiving an authentication response from the remote system; and transferring the authentication response to the payments processor (see at least abst. & col. 1, lines 14-49).

Referring to claim 7, Cook et al. discloses means for generating a digest by performing a hash on the electronic fund transfer disbursement file (see at least abst. & col. 1, 2, lines 14-49, 39-55);

- means for transferring the digest to the remote system (see at least abst. & col. 1, 2, lines 14-49, 39-55);
- means for receiving an authorization response from the remote system, the authorization response comprising a digital signature of authenticated attributes, the authenticated attributes comprising the digest (see at least abst. & col. 1, 2, lines 14-49, 39-55);

Cook et al. does not expressly disclose means for transferring an electronic funds submission to the payments processor over a secure connection, the electronic funds submission comprising

the payment transaction file and at least a portion of the authorization response comprising the digital signature.

Yacobi et al. discloses means for transferring an electronic funds submission to the payments processor over a secure connection, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising the digital signature (see at least abst. & col. 3, lines 57-64).

Therefore, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have modified of Cook et al. to include the step(s) taught by Yacobi et al. as discussed above in order to provide a real-time software application is provided that allows consumers to authorize transaction in a secure, private, and convenient manner for the purchase of goods and services over the internet (see at least col. 1, lines 52-56).

Referring to claim 8, Cook et al. disclose the remote system comprises means for: generating additional message attributes (col. 2, lines 38-65);

- combining the additional message attributes with the digest to generate the authenticated attributes (see at least abst. & col. 2, lines 38-65);
- the digital signature comprises a digital signature of a hash of the authenticated attributes (see at least abst. & col. 2, lines 38-65).

Referring to claim 9, Cook et al. discloses generating and passing a dummy data file to a signing component to obtain a dummy authentication data structure, the dummy authentication data structure comprising a dummy digital signature (see at least abst. & col. 1, lines 14-49);

- passing the authenticated attributes to the signing component to obtain the digital signature (see at least abst. & col. 1, lines 14-49);

- combining the digital signature with at least a portion of the dummy authentication data structure by replacing the dummy digital signature with the digital signature to generate an authentication data structure (see at least abst. & col. 1, lines 14-49);
- including the authentication data structure in the authorization response (see at least abst. & col. 1, lines 14-49).

Referring to claim 10, Cook et al. discloses the dummy data structure further comprises a dummy digest (see at least abst. & col. 1, lines 14-49);

- the remote system further combines the digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest (see at least abst. & col. 1, lines 14-49).

Referring to claim 11, Cook et al. discloses obtaining log on credentials identifying the user of the remote system; determining whether the log on credentials match those of an authorized user (see at least abst. & col. 1, lines 14-49);

- transferring the authorization request to the remote system occurs only if the log on credentials match those of an authorized user (see at least abst. & col. 1, lines 14-49).

Referring to claim 12, Cook et al. discloses receiving an authentication challenge from the payments processor; transferring the authentication challenge to the remote system (see at least abst. & col. 1, lines 14-49);

- receiving an authentication response from the remote system; and transferring the authentication response to the payments processor (see at least abst. & col. 1, lines 14-49).

Referring to claim 13, Cook et al. discloses generate additional message attributes (see at least abst. & col. 1, lines 24-41);

- combine the additional message attributes with the digest to generate the authenticated attributes (see at least abst & col. 1, lines 24-41);
- the digital signature comprises a digital signature of a hash of the authenticated attributes (see at least abst. & col. 1, lines 24-41).

Referring to claim 14, Cook et al. discloses generate and pass a dummy data file to a signing component to obtain a dummy authentication data structure, the dummy authentication data structure comprising a dummy digital signature (see at least abst. & col. 1, lines 14-49);

- pass the authenticated attributes to the signing component to obtain the digital signature (col. 1, lines 14-49);
- combine the digital signature with at least a portion of the dummy authentication data structure by replacing the dummy digital signature with the digital signature to generate an authentication data structure (see at least abst. & col. 1, lines 14-49);
- include the authentication data structure in the authorization response (see at least abst. & col. 1, lines 14-49).

Referring to claim 15, Cook et al. discloses the dummy data structure further comprises a dummy digest (see at least abst. & col. 1, lines 14-49);

- the authorization control code further drives the remote system to combine the digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest (see at least col. 1, lines 14-49).

Referring to claim 16, Cook et al. discloses obtaining log on credentials identifying the user of the remote system (see at least abst & col. 1, lines 14-49);

- determining whether the log on credentials match those of an authorized user (see at least abst. & col. 1, lines 14-49);
- transferring the authorization request to the remote system occurs only if the log on credentials match those of an authorized user (see at least col. 1, lines 14-49).

Referring to claim 17, Cook et al. discloses transferring the authentication response to the payments processor (see at least abst & col. 1, lines 14-49).

Cook et al. does not expressly disclose receiving an authentication challenge from the payments processor; transferring the authentication challenge to the remote system; receiving an authentication response from the remote system.

Yacobi et al. discloses receiving an authentication challenge from the payments processor (see at least col. 1, 5, lines 24-44, 50-57);

- transferring the authentication challenge to the remote system(see at least abst & col. 1, 5, lines 24-44, 50-57);
- receiving an authentication response from the remote system (see at least col. 1, 5, lines 24-44, 50-57).

Therefore, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have modified of Cook et al. to include the step(s) taught by Yacobi et al. as discussed above in order to provide a real-time software application is provided that allows consumers to authorize transaction in a secure, private, and convenient manner for the purchase of goods and services over the internet (see at least col. 1, lines 52-56).

5. **Examiner's Note**: The Examiner has pointed out particular references contained in the prior art of record within the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Response to Arguments

6. Applicant's arguments filed December 03, 2007 have been fully considered but they are not persuasive.

As per claim 1, Applicant argues "Cook does not teach all relate to performing a hash function or generating a digest of an electronic fund transfer disbursement file" (response page 8). As indicated in the abstract of Cook, "The consumer digitally signs the charge slips and encrypts the charge slip and consumer digital sign with a payment key", as in a hash function (also see column 2, lines 40-42).

Further applicant argues "Cook does not teach the step of obtaining a digital signature and generating an authorization response (response page 8)". Cook teaches that upon authorization the digital system of both parties send an authorization message (see column 2, lines 43-51).

Further applicant also argues "Cook does not teach the remote system perform is to generate the authentication response for transmission back to the system, the authorization

response include the digital signature (response page 10). Cook teaches the authorization the digital system of both parties send an authorization message (see column 2, lines 43-51).

As per claim 2, Applicant argues "Cook does not teach a remote system being driven to perform any steps by authorization control code that is provided by a web server and further driving the remote system to generate additional message attributes and combine the additional message attributes with the digest to generate the authenticated attribute (response page 11)". Cook teaches that the authorization the software programs that operate a given Web site and internet merchant sites are targets for hackers who may be able obtain access this data (see column 1, lines 24-35).

As per claim 3, Applicant argues, "Cook does not teach authorization control code further driving the remote system to perform the steps recited (response page 11)". Cook teaches that the authorization the software programs that operate a given Web site and internet merchant sites are targets for hackers who may be able obtain access this data (see column 1, lines 24-35).

As per claim 4, Applicant argues, "Cook does not discuss any steps similar to combining a digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest (response page 12). Cook teaches that the merchant, in turn, uses this information to obtain a transaction approval from a charge card authentication processor. The transmission of data from a purchaser's computer or terminal to the merchant Web site is generally protected by encryption (see column 1, lines 18-23).

As per claim 7, Applicant argues, "Cook does not teach means for generating a digest by performing a hash on the electronic fund transfer disbursement file, transferring the digest the digest to the remote system, and receiving an authorization response from the remote system, the

authorization response comprising a digital signature of the authentication attributes, the authenticated attributes comprising the digest (response pages 12, 13)". Cook teaches that the charge approval services and all incoming charge slips are decrypted, validated by the hash and authenticated by verifying the digital signatures of both the merchant and the consumer. Upon receiving the approval or authentication, the central repository sends the authorization (see column 2, lines 39-50).

Further applicant argues, "Cook does not teach for generating a digest by performing a hash on the electronic fund transfer disbursement file (response page 12)". Cook teaches the consumer digitally signs the charge slips and encrypts the charge slip and consumer digital sign with a payment key (also see column 2, lines 40-42).

Further applicant also argues, "Yacobi does not teach for transferring an electronic funds submission to the payments processor over a secure connection, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising the digital signature (response page 13, 15)". Yacobi teaches that the cpu has a processor and may have a cryptographic acceleration. The cpu is capable of performing cryptographic function, such as signing encrypting, decrypting, authenticating with acceleration (see column 16, lines 8-14).

As per claim 13, Applicant argues, "Cook does not include any teaching of authorization control code that is at least one of executable by the remote system to perform any steps (response pages 15)". Cook teaches that the authorization the software programs that operate a given Web site and internet merchant sites are targets for hackers who may be able obtain access this data (see column 1, lines 24-35).

As per claim 15, Applicant argues, "Cook does not teach that the authorization control code passed to the remote system additionally drives the remote system to perform at least one additional distinctive steps (response pages 15-16). Cook teaches that central repository formats an authorization message containing the required information to obtain a charge card authorization on behalf of both the consumer and the merchant and then forwards the message to a charge card processor (see column 2, lines 42-50).

Conclusion

7. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shahid Kamal whose telephone number is (571) 270-3272. The examiner can normally be reached on MONDAY through THURSDAY between the hours of 8:30 AM and 7 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew J. Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300 for Regular/After Final Actions and 571-273-6714 for Non-Official/Draft.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov.

Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shahid Kamal
January 22, 2008

/Bradley Bayat/
Primary Examiner, Art Unit 3621